Susan Fahringer (SBN 162978)
sfahringer@perkinscoie.com
Nicola Menaldo (*pro hac vice*)
nmenaldo@perkinscoie.com
PERKINS COIE LLP
1301 Second Avenue, Suite 4200
Seattle, WA 98101
Telephone: (206) 359-8687
Facsimile: (206) 359-9000

Caroline Sundermeyer (SBN 353219)
CSundermeyer@perkinscoie.com
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304
Telephone: (650) 838-4300
Facsimile: (650) 838-4350

Attorneys for Defendant The Trade Desk, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

In re The Trade Desk, Inc. Data Privacy Litigation

Case No. 3:25-cv-2889 (CRB)

DEFENDANT THE TRADE DESK, INC'S NOTICE OF MOTION AND MOTION TO DISMISS

Judge: Hon. Charles R. Breyer

DATE: December 5, 2025
TIME: 10:00 a.m.
CTRM: 6, 17th Floor

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on December 5, 2025, at 10:00 am or as soon as thereafter as the matter may be heard, Defendant The Trade Desk, Inc. ("TTD") will bring for hearing in Courtroom 6 (17th Floor) of the above-captioned court located at 450 Golden Gate Avenue, San Francisco, California 94102, a Motion seeking an Order to Dismiss the Consolidated Class Action Complaint in its entirety.

STATEMENT OF RELIEF SOUGHT

TTD moves to dismiss Plaintiffs' Consolidated Class Action Complaint ("CCAC") pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(6) because Plaintiffs fail to satisfy the basic pleading standards required to state a claim for relief. This Motion is based upon this Notice of Motion, the supporting Memorandum of Points and Authorities, the Declaration of Susan Fahringer ("Fahringer Decl.") and attached exhibits, the pleadings and other papers on file herein, and upon such oral argument as the Court may entertain at the hearing on this Motion.

STATEMENT OF ISSUES & SUMMARY OF ARGUMENT

This case targets TTD's participation in the online advertising industry through TTD's use of commonplace website technologies and the services it provides to help advertisers bid for online advertising space. What TTD does is neither unusual nor a violation of the law.

Plaintiffs' privacy claims, asserted under the California Constitution and common law (First and Second Causes of Action), should be dismissed because Plaintiffs have not alleged facts showing that they had a reasonable expectation of privacy or that TTD's conduct constitutes an egregious breach of social norms. *See Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35–40 (1994). Finding TTD's conduct privacy-invasive and highly offensive would be irreconcilable with the California Consumer Privacy Act ("CCPA"), the comprehensive, landmark legislation that permits the very practices that Plaintiffs challenge here. Nor have Plaintiffs plausibly alleged that TTD engages in anything other than routine commercial behavior. Rather, their claims challenge ubiquitous commercial conduct and technologies used across the online advertising industry. *See Hubbard v. Google LLC*, 2024 WL 3302066, at *7

(N.D. Cal. July 1, 2024).

Plaintiffs' wiretapping claims under the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.* ("ECPA") and California Invasion of Privacy Act, Cal. Penal Code § 630 *et seq.* ("CIPA") (Third and Fourth Causes of Action) should be dismissed because (a) Plaintiffs do not plausibly allege that TTD collects the "contents" of their "communications," essential elements of a claim under ECPA or CIPA, *see, e.g.*, *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014), and (b) Plaintiffs do not plausibly allege that TTD "intercepts" any communication while it is "in transit," *see Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. 2002). Additionally, Plaintiffs' ECPA claim should be dismissed because ECPA is a one-party consent statute. Plaintiffs' ECPA claim is therefore barred because at least one party to the communication—the websites with which Plaintiffs were allegedly communicating—consented to any alleged interception. *See* 18 U.S.C. § 2511(2)(d).

Plaintiffs' claim under CIPA's pen register provision (Fourth Cause of Action) should be dismissed because, as the statute's legislative history and intent make clear, Plaintiffs have not alleged facts establishing TTD's use of a "pen register." Pen registers are devices that record *outgoing* information, which is not the data allegedly supporting this claim. *See United States v. New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977). The claim also fails to satisfy the requirements of Rule 8.

Plaintiffs' claim under the California Comprehensive Data Access and Fraud Act ("CDAFA") (Fifth Cause of Action) should be dismissed because CDAFA's private right of action is limited to those "who suffer[] damage or loss," and the loss alleged here does not qualify. Cal. Penal Code § 502(e)(1); *see also Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021). Plaintiffs also fail to allege facts establishing essential elements of this claim, including that TTD acted "without permission," caused damage recognized by the statute, or introduced computer contaminants.

In addition, because ECPA, CIPA, and CDAFA are criminal statutes, the rule of lenity requires any ambiguity regarding the statutes' applicability to be resolved in TTD's favor.

Plaintiffs' unjust enrichment claim (Sixth Cause of Action) should be dismissed because

unjust enrichment is not a standalone cause of action, *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015), the relationship between Plaintiffs and TTD is too attenuated (by Plaintiffs' own admission, it is nonexistent) to support such a claim, *Doe I v. Wal-Mart Stores, Inc.*, 572 F.3d 677, 685 (9th Cir. 2009), and Plaintiffs have not alleged that they lack an adequate remedy at law.

Plaintiffs' declaratory relief claim (Seventh Cause of Action) fails because that is a form of relief, not an independent basis for recovery. *Muhammad v. Conner*, 2012 WL 2428937, at *3 (N.D. Cal. June 26, 2012).

DATED: September 2, 2025

PERKINS COIE LLP

By: */s/* Susan Fahringer
Susan Fahringer
Nicola Menaldo
Caroline Sundermeyer
PERKINS COIE LLP

Attorneys for Defendant The Trade Desk, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This case is about online advertising and the commercial ecosystem that supports it. That ecosystem has been in place for decades and includes hundreds of thousands of businesses—those that sell online ad space, or buy it, or that support those that do. TTD is in the third group: it helps advertisers bid for online ad space and offers a self-service platform to help them do so.

Online advertising makes it possible for websites to make their content available for free. So commonplace is online advertising that seven years ago, California passed comprehensive, landmark legislation, the California Consumer Privacy Act ("CCPA"), to provide a framework to regulate the activity at issue in this case and simultaneously protect Californians' constitutional right to privacy. That framework requires websites to post specific notices about their sharing of personal information for targeted advertising purposes and expressly grants Californians the right to opt *out* of that sharing, along with several related rights. The entire CCPA, along with its extensive implementing regulations, rests upon this opt-out framework.

Plaintiffs do not contend they exercised their opt out rights under the CCPA or that TTD violated that Act—they instead assert that they have "no obligation" to exercise those rights. CCAC ¶ 194. They reject even an opt-*in* framework, one that would require their advance consent before their information is collected, calling it "farcical." *Id.* ¶¶ 153, 163. Plaintiffs claim that unless TTD ceases its "tracking practices"—the very same conduct that is practiced by most of the online advertising ecosystem and regulated by the CCPA—they will have no choice but to "forego use of the internet altogether." *Id.* ¶¶ 3, 211.

The CCAC should be dismissed. Plaintiffs' privacy claims fail because TTD's legislatively endorsed, commonplace activities are not "highly offensive" and do not invade upon any reasonable expectation of privacy. Plaintiffs' wiretap and pen register claims fail because those Cold War-era criminal statutes do not apply. The wiretap claims fail because the data at issue are not the "contents" of "communications," and TTD's conduct is not an "interception" while the data were "in transit." Plaintiffs' pen register claim fails because it is insufficiently pleaded and because California's pen register statute does not apply to the type of

data and conduct at issue here. Plaintiffs' CDAFA claim fails because that statute was intended to prohibit computer hacking that causes tangible harm, which is not alleged here. Plaintiffs' unjust enrichment claim fails because unjust enrichment is not a standalone claim, it applies only where the relationship between the parties is more direct than the one alleged here, and Plaintiffs have not alleged they lack an adequate remedy at law. And Plaintiffs' declaratory relief claim should be dismissed because declaratory relief is not a claim but a remedy.

II. BACKGROUND

A. The Online Advertising Ecosystem

Hundreds of thousands of entities participate in the online advertising industry. Some supply advertising space (*e.g.*, websites, connected TVs, mobile applications) ("publishers"); others ("advertisers") buy it. CCAC ¶¶ 69–70 & n.14. Still others, including TTD, serve in support roles. *Id.* ¶ 108.

Real-Time Bidding. Online ad space is bought and sold primarily through Real-Time Bidding ("RTB") auctions, which have taken place for many years and occur "trillions" of times per year. *Id.* ¶¶ 69–71. Publishers initiate RTB auctions by sending "bidstream data" to a "demand side" platform, a place where advertisers can place bids for that ad space. TTD is one of the many companies that provide demand side platforms. *Id.* ¶¶ 70, 110. Because RTB auctions occur nearly instantaneously (*id.* ¶ 6), they allow a different ad to be displayed depending on when, where, and by whom the ad is being viewed. *See id.* ¶¶ 6, 69. So the bidstream data that publishers introduce into auctions includes information about where the ad will be shown, together with information about who will see it, including the viewers' IP address and type of device. *See id.* ¶¶ 108, 113. Advertisers and the companies that support them (like TTD) typically analyze this bidstream data, along with other data provided by third parties, to decide whether and how much to bid for that ad space and what ad to place. *See id.* ¶¶ 70, 126.

TTD's Data Marketplace. TTD also hosts a "Data Marketplace," where third parties can offer data about potential audiences for ads, which the third parties organize into audience "segments" that reflect potential consumer preferences or characteristics. *See id.* ¶¶ 131–34. TTD's advertiser clients can access this third party "segment" or "audience" data to decide what

ads to show and how much to bid when the advertisers place bids on ad space.[1] *Id.* ¶¶ 1, 70–72, 126; *see also* Declaration of Susan Fahringer ("Fahringer Decl."), Ex. A.[2]

Website Analytics Technologies. TTD also uses standard website technologies found on virtually every website or connected device: cookies, pixels, and SDKs. These technologies help participants in the online advertising ecosystem correlate and organize data about website visitors. Cookies are pieces of software code that store information about website visitors across visits. CCAC ¶ 88. Plaintiffs allege that TTD makes a cookie available to website owners that, when present on websites, assigns a unique Trade Desk ID ("TDID") to allow TTD "to recognize web browsers across sites over time." *Id.*; *see also id.* ¶ 37(a). TTD allegedly "syncs" its cookie IDs to others' cookie IDs ("cookie syncing") to "cross-correlat[e]" information collected through the two cookies. *Id.* ¶¶ 89–93. Pixels are "JavaScript tracking tag[s]" (*id.* ¶ 94) or small pieces of code (*id.* ¶ 99) included in a website's software code. Plaintiffs' claims are based on three TTD pixels: Match Tag, the Universal Pixel, and Static Tracking Pixels. *Id.* ¶ 91. Plaintiffs allege that TTD incorporates information collected through cookies and pixels into "profiles" about them. *See, e.g.*, *id.* ¶¶ 2, 65. An SDK (a software development kit) is ready-made code that software developers can use to make certain tasks easier, like integrating an app with a platform. Plaintiffs' claims are based on TTD's "Real Time Conversion Events" SDK, which Plaintiffs allege makes it easier for software developers to program their apps to send data about user interactions (like page views) to TTD. *Id.* ¶¶ 87, 104, n.45.

---

[1] The CCAC is replete with inaccurate information about TTD's technologies, among other things; TTD accepts its allegations as true solely for the purposes of this motion.

[2] Plaintiffs repeatedly cite to and rely upon TTD's website, as well as the website for Unified I.D. 2.0 (discussed below), throughout the CCAC. *See* Fahringer Decl. ¶¶ 2–6; *see also* CCAC nn.20, 23–24, 27, 53, 128. Exhibits B through E to the Fahringer Declaration are webpages cited by Plaintiffs, and Exhibit A is the master webpage for TTD's platform. These documents are incorporated by reference into the CCAC, and the Court therefore can consider them. *See Knievel v. ESPN*, 393 F.3d 1068, 1076–77 (9th. Cir. 2005); *Lee v. City of L.A.*, 250 F.3d 668, 688 (9th Cir. 2001); *Love v. Handerly Hotels, Inc.*, 2021 WL 2531090, at *3 (N.D. Cal. June 21, 2021) (finding that "publicly-accessible web pages" that the plaintiff "expressly cites" in the complaint were incorporated by reference).

Unified ID 2.0 ("UID2"). TTD developed a free, open-source system for developing identifiers, Unified ID 2.0 (or "UID2"), that is used across the internet. *See* Fahringer Decl., Ex. C; *see also id.* Ex. D; CCAC ¶ 75. UID2 enables participants in the online advertising industry to share information about users' online activity without exposing consumers' email addresses or phone numbers. *See* Fahringer Decl. Ex. C (cited at CCAC n.128); CCAC ¶ 275(a). UID2 is used only for online advertising, and anyone can opt out of "being served targeted ads tied to their UID2" at any time. *See* Fahringer Decl., Ex. E (cited at CCAC n.24); *see also* Fahringer Decl. Ex. B (referencing the "universal UID2 opt-out") (cited at CCAC n.20). Use of UID2 is common and widespread. *See, e.g.*, CCAC ¶ 150 (Disney, Comcast, Warner Bros., and others allegedly use UID2).

B. The Legal Framework Regulating Online Advertising

A comprehensive legal and regulatory framework, anchored by California's landmark privacy law, the CCPA, protects California consumers' constitutional right to privacy in the online advertising setting and covers the very conduct and data at issue here.[3] The CCPA requires businesses that collect personal information from consumers to provide specific notice of their practices involving "sharing" and "selling"[4] of consumers' personal information for online advertising purposes, and to allow consumers the opportunity to opt *out* of such practices.[5] Cal. Civ. Code § 1798.120(a). The entire CCPA, and the online advertising ecosystem it

---

[3] *See* Cal. Civ. Code § 1798.140(v)(1) (covered data includes "identifiers such as a … unique personal identifier, online identifier, Internet Protocol address, email address … or other similar identifiers," "browsing history," "information regarding a consumer's interaction with an Internet Web site, application, or advertisement," and associated profiles); *see also* Cal. Code Regs. tit. 11, § 7025(c) ("opt-out" rights apply to "any consumer profile associated with [a] browser or device, including pseudonymous profiles").

[4] *See* AB 375, 2017–2018 Reg. Sess. (Cal. 2018); Cal. Civ. Code § 1798.140(ad) ("sale" includes "making available" personal information).

[5] *See* Cal. Code Regs. tit. 11, § 7025(c) ("opt-out" rights apply to "any consumer profile associated with [a] browser or device, including pseudonymous profiles"). The CCPA grants Californians additional rights, as well, including the right to access the data collected about them (including inferences therefrom) and the right to request deletion of that data. *See, e.g.*, Cal. Civ. Code §§ 1798.110, 1798.130.

regulates, rests on this opt-*out* foundation. The legislature later considered, but did not enact, an advance consent, "opt-*in*" framework like that adopted in the EU. *See* Assemb. Comm. on Privacy & Consumer Prot., Analysis of A.B. 1760, 2019–2020 Reg. Sess. (Cal. Apr. 23, 2019); *see also* CCAC ¶ 163.

The voter-initiated California Privacy Rights Act (CPRA) amended the CCPA in 2020. Among other things, the amendments expressly made clear that the CCPA's protections apply to "cross-context behavioral advertising" (selecting what ads to show a consumer based on their activity across multiple websites or online services) and created the California Privacy Protection Agency ("Agency"), whose sole mission is to protect the privacy of California consumers. The Agency subsequently promulgated detailed regulations that lay out how consumers may easily opt out of the sale or sharing of their personal information—including through "opt out preference signals" through which California consumers may opt out of the selling and sharing of their personal information by *all* businesses with a single act—and how businesses must ensure that they honor these signals. *See* Cal. Civ. Code § 1798.140(k); Cal. Code Regs. tit. 11, § 7013. The Agency and California Attorney General actively enforce the CCPA and its corresponding regulations and can impose stiff penalties for violations. *See* Cal. Civ. Code § 1798.199.90.

C. Plaintiffs' Claims

Plaintiffs reject the foundational opt-*out* based legal framework for online advertising in California. They also reject the EU's opt-*in* framework as "farcical" (CCAC ¶ 163) and contend that consent is not "reasonably possible or practical," *id.* ¶¶ 3, 153. Plaintiffs acknowledge that the conduct they challenge in this lawsuit is practiced routinely by businesses across the web, trillions of times a year, yet Plaintiffs seek an injunction prohibiting that conduct as well as substantial damages. *See, e.g.*, *id.* ¶¶ 154, 163, 211.

Plaintiffs assert seven claims, each based on different TTD conduct or technologies: invasion of privacy, intrusion upon seclusion, violation of ECPA, violation of CIPA §§ 631 and 638.51 (state wiretap and pen register statutes), violation of CDAFA, unjust enrichment, declaratory relief. Plaintiffs seek to represent a California class for their invasion of privacy,

ECPA, CIPA, and CDAFA claims (First, Third, Fourth, and Fifth Causes of Action), nationwide classes for their intrusion upon seclusion and declaratory judgment claims (Second and Seventh Causes of Action), and nationwide and California classes, in the alternative, for their unjust enrichment claim (Sixth Cause of Action). *See generally id.*

III. LEGAL STANDARD

A complaint must contain sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "[A] sheer possibility that a defendant has acted unlawfully" is not enough. *Id.* Courts do not assume the truth of legal conclusions pleaded as factual allegations. *Id.* at 677–79; *Bell Atl. v. Twombly*, 550 U.S. 544, 555 (2007).

IV. ARGUMENT

A. Plaintiffs' privacy claims fail because they have not pleaded a reasonable expectation of privacy or that TTD's conduct was highly offensive.

"The California Constitution sets a 'high bar' for establishing an invasion of privacy claim." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014). Plaintiffs must plead: (1) a reasonable expectation of privacy under the circumstances; and (2) a highly offensive invasion of that privacy constituting "an egregious breach of . . . social norms." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35-40 (1994). Because the "right to privacy in the California Constitution sets standards similar to the common law tort of intrusion [upon seclusion]," the two claims are analyzed together. *See Hernandez v. Hillsides*, 47 Cal. 4th 272, 275 (2009). Courts regularly resolve invasion of privacy claims as a matter of law at the pleading stage. *See McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *7 (N.D. Cal. Feb. 2, 2021) (collecting cases). Plaintiffs here cannot clear the high bar imposed by the California Constitution, so their claims fail as a matter of law.

1. Plaintiffs do not plausibly allege a reasonable expectation of privacy.

The reasonable expectation of privacy inquiry asks whether a plaintiff's purported "expectation of privacy is reasonable in the particular setting or context at issue." *Matthews v. Becerra*, 8 Cal. 5th 756, 770 (2019); *see also Hernandez*, 47 Cal. 4th at 286. Under California

law, "sources of positive law governing the right to privacy," like "statutory enactment" and "ballot arguments" factor into whether a stated expectation of privacy is reasonable. *Hill*, 7 Cal. 4th at 36. Here, when the California legislature initially enacted the CCPA, and when the people of California voted to amend it, both acknowledged the very practices challenged in the CCAC, yet neither banned them nor required opt-in consent. *See, e.g.*, Cal. Prop. 24 (California Privacy Rights Act), Gen. Elec., Nov. 3, 2020 (amending Cal. Civ. Code § 1798.100 *et seq*.) § 3(C) (recognizing that "advertising businesses . . . track [consumers] across the internet, and . . . create detailed profiles of their individual interests"). And the CCPA—passed by California voters and legislatures representing Plaintiffs—governs the very right to privacy that Plaintiffs claim has been violated. AB 375, 2017–2018 Reg. Sess. (Cal. 2018) § 2(a) (noting that "[f]undamental to [the] right of privacy is the ability of individuals to control the use, including the sale, of their personal information"); *Gutierrez v. Converse Inc.*, 2025 WL 1895315, at *3 (9th Cir. July 9, 2025) (Bybee, J., concurring) (affirming the dismissal of privacy claims based on online activity and noting that "plaintiffs . . . are not without recourse, thanks to the [CCPA]" which "likely covers the allegations here"). Because the CCPA expressly *permits* and regulates the very conduct that underlies Plaintiffs' claims, Plaintiffs cannot have had a reasonable expectation that TTD *would not* engage in that conduct.

Additionally, and as several courts have recognized, online tracking is ubiquitous and well-understood, diminishing any reasonable expectation of privacy online. *See Thomas v. Papa Johns Int'l, Inc.*, 2024 WL 2060140, at *1 (S.D. Cal. May 8, 2024) ("[T]he internet is not a place where users have a reasonable expectation of privacy."), *aff'd*, 2025 WL 1704437 (9th Cir. June 18, 2025); *Hubbard v. Google LLC*, 2024 WL 3302066, at *7 (N.D. Cal. July 1, 2024). (dismissing invasion of privacy claim alleging the collection of browsing data because "contemporary internet browsing involves the collection of users' data, including by tracking users across the internet, and a reasonable user should expect as much"). Plaintiffs themselves acknowledge that the "RTB process occurs 178 trillion times annually across the U.S. and Europe," and through that process, bidstream data is shared with "untold numbers" of RTB participants. CCAC ¶¶ 3, 71. Plaintiffs have not plausibly alleged that they could have

reasonably believed that their internet activity would be exempted from these widespread practices.[6] *See id.* ¶ 162.

This case bears little resemblance to those where courts have found a reasonable expectation of privacy in the internet context. Those cases typically involve a direct connection between the parties as well as a showing that the plaintiff was deceived or that the defendant breached a privacy-related promise to them. In *In re Facebook, Inc. Internet Tracking Litigation*, for example, the plaintiffs were Facebook users, and the "critical fact" giving rise to a reasonable expectation of privacy was that Facebook affirmatively *misrepresented to them* "that logged-out user data would not be collected." 956 F.3d 589, 602-03 (9th Cir. 2020). But here, Plaintiffs concede that they have no connection with TTD, and they do not allege that they were deceived by TTD or that TTD breached any promises made to them. *See* CCAC ¶¶ 67, 157 (no relationship to TTD); *see also Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1090–91 (N.D. Cal. 2022) (distinguishing *In re Facebook* because "Facebook's surreptitious data collection contravened its affirmative promises").

Instead, Plaintiffs' case is far more like those in which plaintiffs have failed to establish privacy claims because they allege nothing more than the collection of online browsing data without consent. As those cases have held, there is no reasonable expectation of privacy in that type of online data. *See Jones v. Peloton Interactive, Inc.*, 720 F. Supp. 3d 940, 951 (S.D. Cal. 2024) ("[t]he collection of users['] information concerning various fitness products and services

---

[6] Nor can Plaintiffs claim a reasonable expectation of privacy in the segment data allegedly available through TTD's data marketplace, because they do not allege any facts about the *context* in which the information was allegedly collected from them. That is fatal to their claims because attributes about a person (such as their support for the war in Ukraine, CCAC ¶ 12) may be private or public depending on the context. *See Virgil v. Time, Inc.*, 527 F.2d 1122, 1126 (9th Cir. 1975). If a Plaintiff believes some attribute about them is private, they must allege that with more specificity than they have done here, including the context in which it was collected. *See B.K. v. Eisenhower Med. Ctr.*, 721 F. Supp. 3d 1056, 1064 (C.D. Cal. 2024) (dismissing privacy claims because the 90-page complaint "fail[ed] to allege any specificity as to what medical information was allegedly disclosed or when it was disclosed"), *reconsideration in part on other grounds*, 2024 WL 203404 (C.D. Cal. Apr. 11, 2024).

shared on the chat" is "routine commercial behavior"); *Seedy v. Microsoft Corp.*, 2023 WL 8828852, at *4 (W.D. Wash. Dec. 21, 2023) (plaintiffs "have no recognized reasonable expectation of privacy in their browsing data"); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 524–25 (C.D. Cal. 2021) (plaintiff did not have "a reasonable expectation of privacy over his activity on [defendant's] Website"); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (disclosure to third party of user's browsing history URLs and unique ID could not give rise to invasion of privacy claim). Plaintiffs' privacy claims should be dismissed as a matter of law for similar reasons because they have not pleaded a reasonable expectation of privacy in the data at issue.

2. Plaintiffs do not plausibly allege that TTD's conduct was "highly offensive."

The "highly offensive" inquiry turns on whether the violation constitutes "an egregious breach of the social norms." *In re Facebook.*, 956 F.3d at 601; *Mastel v. Miniclip S.A.*, 549 F. Supp. 3d 1129, 1137 (E.D. Cal. 2021). Plaintiffs' allegations establish the opposite.

Democratically enacted laws reflect the relevant "social norms" that guide the "highly offensive" analysis, which focuses on whether the alleged "intrusion is unacceptable as a matter of public policy." *See Hammerling*, 615 F. Supp. 3d at 1090 (citation omitted). Indeed, "statutes" can "defin[e] . . . what constitutes 'egregious' or highly offensive conduct." *Mastel*, 549 F. Supp. at 1139; *see also Romero v. Dep't Stores Nat'l Bank*, 725 F. App'x 537, 540 (9th Cir. 2018) (a statute that proscribes specific conduct and provides for civil penalties "suggest[s] that the California legislature and other reasonable people could consider such conduct highly offensive").[7] Here, the CCPA codifies the relevant "social norms" and *permits* the very conduct Plaintiffs claim is highly offensive, including the tracking and sharing of online activity and the creation of profiles. *See supra*, Section II.B. Such activity therefore cannot be an "egregious

[7] Notably, the court in *Riganian v. LiveRamp Holdings, Inc.*, 2025 WL 2021802, at *7 (N.D. Cal. July 18, 2025) did not mention the CCPA in its "highly offensive" analysis, much less consider whether plaintiffs' invasion of privacy theory could coexist with that comprehensive privacy statute.

breach of . . . social norms." *In re Facebook*, 956 F.3d at 601.

Courts analyzing whether conduct is "highly offensive" also assess the defendant's "motives and objectives" and "whether countervailing interests . . . render the intrusion inoffensive." *Hammerling*, 615 F. Supp. 3d at 1090 (citation omitted). Both factors weigh heavily in TTD's favor. Plaintiffs do not plausibly allege illicit motives; to the contrary, they concede that TTD collects data to help its clients bid effectively on ad space online. CCAC ¶ 72. As the Ninth Circuit recently confirmed, "tracking . . . [online] interactions" is a purely commercial, legal endeavor and is not the "kind of harm that is remotely similar to the 'highly offensive' interferences or disclosures that were actionable at common law." *Popa v. Microsoft Corp.*, 2025 WL 2448824, at *5 (9th Cir. Aug. 26, 2026). Accordingly, courts consistently hold that tracking users online and sharing the accompanying data with third parties—precisely what TTD is alleged to have done here—is "routine commercial behavior," not a "'highly offensive' invasion of privacy." *Hammerling*, 615 F. Supp. 3d at 1090 (collection of sensitive personal data from applications on smartphones not highly offensive).[8]

"Countervailing interests" also confirm that TTD's conduct is not highly offensive. *See Hammerling*, 615 F. Supp. 3d at 1090. The practices Plaintiffs challenge support an online ecosystem that helps keep online content free, including for Plaintiffs themselves. *See, e.g.*, CCAC ¶¶ 67, 69. And Plaintiffs' contention that they will be forced to "forego use of the internet altogether" to protect their privacy (CCAC ¶ 3) is belied by the CCPA. That comprehensive statute gives them "a simple and easy-to-use method by which . . . [they] can opt-out of sale and sharing of their personal information with *all businesses they interact with online* without having

[8] *See also Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1126 (S.D. Cal. 2023) (dismissing invasion of privacy claim because "disclosing a user's browsing history does not plausibly reach the level of 'highly offensive' conduct under either common law or the California Constitution"); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 987–88 (N.D. Cal. 2014) (disclosure of browser history to third parties not highly offensive); *Low*, 900 F. Supp. 2d at 1025 ("The information disclosed to third parties by LinkedIn, including a numeric code associated with a user and the URL of the profile page viewed, does not meet the standard set by California courts."); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosures of unique device identification number, personal data, and geolocation information without consent not an egregious breach of social norms).

to make individualized requests with each business." Cal. Code Regs. tit. 11, § 7025(a) (emphasis added).

Plaintiffs also vaguely allege that TTD collects sensitive information about unspecified "offline activities, such as their geolocation and real-world purchases." CCAC ¶ 203. But this does not change the analysis for a number of reasons. *First*, the CCPA provides an opt out for both sharing *and* the unexpected use of sensitive information. *See* Cal. Civ. Code § 1798.121. *Second*, the allegations are too vague to allow the Court to assess whether the activity is "highly offensive" according to social norms. *See, e.g.*, *Hammerling*, 615 F. Supp. 3d at 1090 (merely alleging "information about a user's religion, political affiliation, or sexual preference does not suffice"); *Jones*, 720 F. Supp. 3d at 951 (allegations that the defendant collects communications "even when such conversations are private and deeply personal" and that "visitors often share highly sensitive personal data" were too vague to state a claim). *Third*, offline activity is highly offensive only if it involves an "exceptional kind of prying into another's private affairs," like "taking the photograph of a woman in the hospital with a 'rare disease that arouses public curiosity'" or "using a telescope to look into someone's upstairs bedroom window for two weeks and taking intimate pictures." *Med. Lab'y Mgmt. Consultants v. Am. Broad. Cos.*, 306 F.3d 806, 819 (9th Cir. 2002). Nothing of the sort is alleged here.

B. Plaintiffs do not state a wiretap claim.

To state a claim under ECPA, Plaintiffs must plausibly allege facts showing that TTD: (1) intentionally (2) intercepted (3) the contents of (4) their electronic communications (5) while in transit (6) using a device. *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1075 (N.D. Cal. 2023). The analysis for a violation of CIPA "is the same as that under the federal Wiretap Act." *See Hammerling*, 615 F. Supp. 3d at 1092. Plaintiffs' ECPA and CIPA claims rest solely on the allegation that TTD's web analytics technologies—the Universal Pixel, static tracking pixel, and Real Time Events SDK—collect data online. *See* CCAC ¶¶ 88–107. But these Cold War-era criminal eavesdropping statutes do not cover the data at issue or the way in which these commonplace technologies work, so Plaintiffs' ECPA and CIPA wiretap claims should be dismissed.

1. Plaintiffs have not plausibly alleged that TTD intercepted the "contents" of their "communications."

To state a wiretap claim, Plaintiffs must first establish that the data at issue were the "contents" of their "communications." *Doe*, 690 F. Supp. 3d at 1075. But here, Plaintiffs allege that TTD's "trackers intercept actions taken, product views, [and] purchase intent . . . taken on websites." CCAC ¶ 222. This confuses *actions* with *communications*. While the wiretapping statutes regulate the latter in certain circumstances, they do not regulate the former, which is the data at issue here. *See Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021) (explaining that unlike "the words of a text message or an email," actions such as "keystrokes, mouse clicks, [and] pages viewed" do not constitute "message content"); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1086 (N.D. Cal. 2018) (similar), *reconsideration on other grounds*, 2018 WL 3068248 (N.D. Cal. June 21, 2018); *Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58, 70 (W.D. Pa. 2023) (similar), *aff'd as modified*, 2025 WL 2250261 (3d Cir. Aug. 7, 2025).

Nor are the data at issue the "contents" of communications, so are not covered by the wiretap statutes. Under ECPA and CIPA, "the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication" such as the "'name,' 'address,' and 'subscriber number or identity' of a subscriber or customer" or the metadata regarding the characteristics of the conversation. *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014).

Plaintiffs' conclusory allegation that the data TTD collects is "the contents of Plaintiffs' communications" (*see, e.g.*, CCAC ¶ 224) is nothing more than a "formulaic recitation of the elements" of a claim and cannot be credited. *See Twombly*, 550 U.S. at 555. Plaintiffs' attempt to bolster that conclusion by alleging "upon information and belief" that TTD intercepts things like "the precise URL being viewed by the user" and "the contents of search queries" fares no better. CCAC ¶ 223. A URL is the location of a web resource, not a message someone communicates. *See, e.g.*, *In re Facebook*, 956 F.3d at 596. Similarly, merely alleging that the "contents of search

queries" were intercepted, without identifying even the search terms used, is not enough. While the *Zynga* court left open the possibility that in some circumstances, URLs revealing a person's search terms *might* constitute the contents of a person's communications, it by no means suggested that a *bare allegation* of search term interception would be enough to withstand a motion to dismiss. *See In re Zynga*, 750 F.3d at 1106; *see also Jones*, 720 F. Supp. 3d at 947 (alleging that "full transcript of the conversation" without facts "about the content" of the conversations insufficient); *Hammerling*, 615 F. Supp. 3d at 1093 (CIPA claim must "identify the specific videos or document that the user views"); *Jones v. Tonal Sys., Inc.*, 751 F. Supp. 3d 1025, 1038 (S.D. Cal. 2024) ("engag[ing] with the chat feature" insufficient); *Hughes v. Vivint, Inc.*, 2024 WL 5179916, at *5 (C.D. Cal. July 12, 2024) (dismissing claims where "[p]laintiff does not clearly allege what personalized information of hers was actually collected").

2. TTD did not read communications that were "in transit."

For a communication to be "intercepted" under ECPA, it must have been "acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). CIPA sets an even higher bar, requiring that a defendant "reads, or attempts to read, or to learn the contents or meaning of any . . . communication while the same is in transit." Cal. Penal Code § 631(a). This language confirms that CIPA is designed to protect interceptions that occur when a third party not only *possesses* a communication but *actively tries to understand* its private message. *See* Cal. Penal Code § 630.

The "in transit" requirement applies with full force in internet cases, where there is necessarily a "narrow window" for interception given the speed at which communications are transmitted. *See NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 951–52 (N.D. Cal. 2014). Failure to demonstrate interception during that narrow window is fatal, because "it would stretch CIPA's statutory language too far to interpret 'while . . . in transit' to encompass any hypothetical future attempt to read or understand the meaning of a communication." *Torres v. Prudential Fin., Inc.*, 2025 WL 1135088, at *6 (N.D. Cal. Apr. 17, 2025).

Plaintiffs allege that the pixels that TTD's partners install on their websites enable TTD to collect URLs reflecting search terms and other related information (CCAC ¶¶ 9, 223), but

TTD's collection necessarily occurs *after* Plaintiffs visit those websites. *See In re Zynga*, 750 F.3d at 1101–02 (when a user enters a URL or interacts with a website, the user's browser (the "client") *then* sends a "GET request" to the website's server, which *then* responds by delivering the requested content); *Griffith v. TikTok, Inc.*, 2024 WL 5279224, at *10 (C.D. Cal. Dec. 24, 2024) (the "sequence" of transmission is determinative for interception claims), *appeal filed*, No. 25-553 (9th Cir. Jan. 28, 2025).

Once again, Plaintiffs' conclusory allegations that TTD's interceptions occurred while Plaintiffs' communications with websites were "in transit," *see, e.g.*, CCAC ¶ 235, are bare recitations of the claim, not entitled to the presumption of truth at the pleading stage. Plaintiffs' wiretap claims should be dismissed because Plaintiffs have not alleged this essential element. *See Mastel*, 549 F. Supp. 3d at 1136 (dismissing CIPA claim for failure to establish "in transit" element); *Rodriguez v. Google LLC*, 2022 WL 214552, at *2 (N.D. Cal. Jan. 25, 2022) (repetition does not cure this problem).

3. The websites, parties to the alleged "communications," consented to any alleged interception.

Plaintiffs' ECPA claim also fails because ECPA is a one-party consent statute. *See* 18 U.S.C. § 2511(2)(d). The parties to the communication at issue here are the websites and the plaintiffs (CCAC ¶ 219), and the websites consented when they placed TTD's code on their websites. Courts routinely dismiss similar claims on this basis. *See Doe I v. Google LLC*, 741 F. Supp. 3d 828, 842 (N.D. Cal. 2024); *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928 (N.D. Cal. 2023).

Recognizing that the websites' consent is fatal to their claims, Plaintiffs assert that such consent is invalid because TTD's alleged interception was carried out "for the purpose of committing any criminal or tortious act." 28 U.S.C. § 2511(2)(d). But the Ninth Circuit has made clear that the "criminal or tortious purpose *must be separate and independent* from the act of the recording." *See Planned Parenthood Fed'n of Am., Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022) (emphasis added); *see also In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 515 (S.D.N.Y. 2001) (the exemption was designed to prevent use of "secret recordings for

insidious purposes" like "blackmail" and "stealing business secrets"). According to Plaintiffs, the alleged criminal or tortious purpose was to "further invad[e] Plaintiffs' . . . privacy." *See* CCAC ¶¶ 238–41. But that is not "separate and independent from the act of the recording"—it is *based* on it. *See Planned Parenthood*, 51 F.4th at 1136. Plaintiffs' bootstrapping argument would cause the consent exception to swallow the rule: any plaintiff could claim that any recording was made to invade their privacy.

In addition, this exception does not apply unless Plaintiffs plausibly alleges that TTD's "*primary motivation* . . . has been to injure plaintiffs tortiously." *Lakes v. Ubisoft, Inc.*, 777 F. Supp. 3d 1047, 1057 (N.D. Cal. Apr. 2, 2025) (quotation marks omitted; emphasis added), *appeal filed*, No. 25-2857 (9th Cir. May 2, 2025). But according to the CCAC, TTD's intent was to "profit[] from the sale of Plaintiffs' . . . personal information." CCAC ¶ 238. This deficiency, too, precludes ECPA's crime-tort exception. *See In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014). *Finally*, TTD's conduct also is not an invasion of privacy and so would not qualify as a tortious act, for the reasons discussed *supra*, Section IV.A.

C. Plaintiffs have not stated a claim for violation of California's pen register statute.

Plaintiffs' pen register claim fails, too, because California's pen register statute does not apply to the conduct at issue here. California's pen register statute requires a court order for the installation and use of a pen register. Cal. Penal Code § 638.51. Only electronic or wire communication service providers, such as websites that provide email and telephone services, can rely on exemptions to the court order requirement. *See id.* § 638.51(b). The statute defines "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information . . . but not the contents of a communication." *Id.* § 638.50(b). To be a pen register, a device must record *outgoing* data, such as "the numbers *dialed* on a telephone," not the caller's own phone number. *See United States v. New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977); Cal. Penal Code § 638.50(b) (a pen register records or decodes "information *transmitted by* an instrument or facility") (emphasis added).

Plaintiffs' pen register claim (CCAC ¶¶ 254–263) is by no means a model of clarity. As far as TTD can tell, Plaintiffs claim that TTD's pixels and SDKs are illegal pen registers because—just like other SDKs and pixels used across the internet—they record "addressing or signaling information" such as "IP addresses." *Id.* ¶ 257. But the alleged recording of IP addresses cannot underpin a pen register claim. That is because an internet user's IP address is the equivalent of a caller's *own* phone number and therefore does not involve the recording of *outgoing information*, as the statute requires. *See Rodriguez v. Plivo Inc.*, 2024 WL 5184413, at *2 (Cal. Super. Ct. Oct. 2, 2024) ("Plaintiff's IP address is not the type of information collected by pen registers" because "[p]en registers collect outgoing information").

Elsewhere, Plaintiffs gesture vaguely at an alternative theory: that TTD's "code, as described at paragraphs 219-235" functions as a pen register because it collects "URLs and email addresses." CCAC ¶ 257. That stray reference to email addresses and URLs gets Plaintiffs nowhere. For one, the cross-referenced descriptions of TTD's code do not mention the collection of email addresses once, so the theory is not well pleaded. Regardless, the alleged recording of Plaintiffs' email addresses cannot serve as the basis of a pen register claim any more than the recording of Plaintiffs' IP addresses can: neither one is *outgoing* information. *See Rodriguez*, 2024 WL 5184413, at *2. Plaintiffs fare no better in their attempt to invoke "URLs." CCAC ¶ 257. The portion of the CCAC Plaintiffs cross-reference contains numerous references to different types of URLs, yet Plaintiffs offer no explanation of which precise URLs and alleged practices support their pen register claim, in violation of Rule 8. Further compounding the notice problem is the fact that Plaintiffs repeatedly assert in that section that the URLs in question are "content" of "communication." *See, e.g.*, CCAC ¶ 231. While "Rule 8 allows pleading in the alternative, the liberal pleading policy has its limits," and Plaintiffs exceed those limits here by attempting to rely on two contradictory theories of liability at the same time. *See Carroll v. Progressive Cas. Ins. Co.*, 2023 WL 3526137, at *5 (C.D. Cal. Mar. 6, 2023).

To be clear, Plaintiffs' theory would require the Court to interpret California's pen register statute to generally require a *court order* before using a "device or process" to "record or decode" IP addresses or URLs. *See* Cal. Penal Code § 638.51. The consequences of adopting this

theory would be staggering. IP addresses and URLs are necessary to route data to the correct destination across the entire internet. And if a device connected to a network could not collect IP addresses or URLs without a court order, then, for example, websites could not be displayed. It would not be enough for someone to consent to the collection, either, because the statutory consent exception applies only to wire or electronic communications service providers. *See id.* § 638.51(b). This cannot have been the intention of the California legislature when it enacted the pen register statute in 2015. Website analytics technologies were commonplace at the time. If those technologies had been the concern of California's pen register statute, then one would expect the legislature to have mentioned them somewhere in the statute's text or legislative history. The legislature did not. *See* A.B. 929, 2015–2016 Reg. Sess. (Cal. 2015). Plaintiffs' pen register claim should be dismissed.

D. Plaintiffs have not stated a CDAFA claim.

CDAFA is an "anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose[s]." *Custom Packaging Supply, Inc. v. Phillips*, 2015 WL 8334793, at *3 (C.D. Cal. Dec. 7, 2015). "As a penal statute," CDAFA "is to be strictly construed." *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 863 (N.D. Cal. 2011); *see also infra*, Section IV.D.2.e. Plaintiffs' CDAFA claim should be dismissed for lack of standing and failure to comply with the pleading requirements of Feder Rules of Civil Procedure 8 and 9(b).

1. Plaintiffs have not alleged the type of loss necessary to confer statutory standing.

Consistent with its anti-hacking purpose, only one "who suffers damage or loss by reason of a violation [of CDAFA] may bring a civil action." Cal. Penal Code § 502(e)(1). Plaintiffs here allege loss of "control" over their "personal information, the ability to receive compensation for their data, and the ability to withhold their data for sale." CCAC ¶ 282. Courts consistently reject this theory of injury under CDAFA. *See, e.g.*, *Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1021 (C.D. Cal. 2023) ("a loss of control over personal data" is not the "injury contemplated by the CDAFA," agreeing "with the majority of courts to consider the issue");

Cottle , 536 F. Supp. 3d at 488 (loss of control, value, and protection of data do not qualify); *Doe v. County of Santa Clara*, 2024 WL 3346257, at *9 (N.D. Cal. July 8, 2024) (same); *Doe*, 690 F. Supp. 3d at 1082 (diminished value not cognizable under CDAFA); *Shah v. Cap. One Fin. Corp.*, 768 F. Supp. 3d 1033, 1048 (N.D. Cal. 2025) (same). Plaintiffs' failure to establish the loss required under CDAFA is fatal to their claim.

2. Plaintiffs have not plausibly alleged essential elements of their CDAFA claims.

Plaintiffs' CDAFA claims also fail on their merits because Plaintiffs have not specifically alleged that TTD (1) acted without permission, (2) damaged their data, or (3) introduced "computer contaminants."

a. Plaintiffs' imprecise and conclusory CDAFA claim should be dismissed under Rules 8 and 9(b).

The CCAC relies on the same jumbled set of allegations to support claims under seven different subsections of CDAFA, even though each of those subsections proscribes different conduct. CDAFA claims sound in fraud, and must be pleaded with Rule 9(b) particularity, which Plaintiffs have plainly failed to do. *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *5 (N.D. Cal. Nov. 20, 2020) (CDAFA claims "sound[] in fraud"); *Bodenburg v. Apple Inc.*, 146 F. 4th 761, 771 (9th Cir. 2025) (under Rule 9(b), plaintiffs must identify the "'who, what, when, where, and how' of the misconduct charged"). Plaintiffs make no effort to tie their prolix factual allegations to the elements of the several CDAFA subsections they claim TTD violated.[9] Plaintiffs' allegations are insufficient under Rules 8 and 9(b) because they fail to give TTD fair notice of the factual basis of their claims.

[9] As one example, Plaintiffs allege that TTD accessed or used their "data, computers computer services, and computer networks" CCAC ¶ 280. Elsewhere, they substitute "computer systems" for "computer services." *Id.* ¶ 277. But these terms mean different things and can affect the viability of claims under different subsections. *Compare* Cal. Penal Code § 502(d)(3) (pertaining only to "computer services") *with* § 502(d)(7) (pertaining to "computer[s], computer system[s], or computer network[s]"); *see also*, *e.g.*, *In re Oliveras*, 103 Cal. App. 5th 771, 780–81 (2024)(dismissing CDAFA claims based on distinctions between terms and among subsections), *as modified on denial of reh'g* (Aug. 2, 2024).

b. Plaintiffs do not allege TTD acted "without permission."

Each of Plaintiffs' CDAFA claims requires a showing that TTD acted "without permission" of the owner of the affected computer, website, or data. *See* Cal. Penal Code § 502(c)(1)–(4), (6)–(8); *Bui-Ford v. Tesla, Inc.*, 2024 WL 694485, at *5 (N.D. Cal. Feb. 20, 2024) (some subsections penalize *access* "without permission" while some subsections penalize other *conduct* "without permission").[10] Plaintiffs vaguely refer to TTD circumventing "privacy-preserving mechanisms," CCAC ¶¶ 152, 277, 280, but do not explain what those are—let alone the who, what, where, when, and how TTD allegedly circumvented them. *See Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1219 (N.D. Cal. 2014) (allegations insufficient where "it [was] not clear *whose* technical or code-based barriers . . . LinkedIn circumvent[ed]" nor "how *LinkedIn* overc[ame] those barriers[]"). Courts have held that "the mere fact that a plaintiff does not consent to an action does not create liability under the CDAFA." *Gutierrez v. Converse Inc.*, 2023 WL 8939221, at *4 (C.D. Cal. Oct. 27, 2023); *see also Facebook*, 2010 WL 3291750, at *11 (plaintiff cannot show "access . . . . without permission simply because [defendant allegedly] violated a contractual term of use"). Plaintiffs' CDAFA claims fail on this basis.

c. Plaintiffs have not alleged that TTD damaged anything.

Plaintiffs' claims under Sections 502(c)(1) and (c)(4) fail because they apply only where a defendant "alters, damages, deletes, destroys, or otherwise uses" any data or device. Cal. Penal Code § 502(c)(1), (c)(4); *Ticketmaster L.L.C. v. Prestige Ent. W., Inc.*, 315 F. Supp. 3d 1147, 1175 (C.D. Cal. 2018). The "otherwise uses" portion of this clause means something *akin to* altering, damaging, or destroying. *McGowan v. Weinstein*, 505 F. Supp. 3d 1000, 1020 (C.D. Cal. 2020). Plaintiffs here have not alleged harm akin to altering, damaging, or destroying data.

[10] Although some courts have rejected the narrower interpretation of "without permission" as requiring that the plaintiff allege the defendant overcame a technical or code-based barrier, *see, e.g.*, *Brown v. Google LLC*, 685 F. Supp. 3d 909, 940 & n.38 (N.D. Cal. 2023), the narrower interpretation is the only reading that avoids the "constitutionally untenable situation in which criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use," *Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010); *see also infra*, Section IV.D.2.e.

They allege only that TTD "accessed[,]" "us[ed,]" "record[ed,]" or "transmit[ted]" their data. CCAC ¶¶ 275, 278. This is not enough.

d. Plaintiffs have not plausibly alleged that TTD introduced computer contaminants.

Section 502(c)(8) prohibits the "introduc[tion of] any computer contaminant." Cal. Penal Code § 502(c)(8). This section is "aimed at 'viruses or worms,' and other malware that usurps the normal operation of the computer or computer system." *In re iPhone Application Litig.*, 2011 WL 4403963, at *13 (N.D. Cal. Sept. 20, 2011). Plaintiffs parrot the statute's language and conclusorily allege that UID2 tokens caused devices to act in a way contrary to what they intended (CCAC ¶ 275), but Plaintiffs do not plausibly or specifically allege that any of TTD's technologies so damaged or "impair[ed] the integrity or availability of" any of their computer systems. *Fidlar Techs. v. LPS Real Est. Data Sols., Inc.*, 810 F.3d 1075, 1084 (7th Cir. 2016); *In re iPhone Application Litig.*, 2011 WL 4403963, at *13. Website analytics technologies, such as TTD's cookies, are ubiquitous and essential to normal operation of the internet and cannot plausibly be characterized as "contaminants." To find otherwise would effectively criminalize the internet. Finally, TTD does not "introduce" anything: TTD receives data from third parties and third-party websites choose to "use and deploy [TTD's technologies] on their platforms." CCAC ¶¶ 77, 277.

E. The Rule of Lenity prohibits accepting Plaintiffs' theories of liability.

If any ambiguity remains regarding whether ECPA, CIPA, or CDAFA apply, the Court must resolve it in TTD's favor under the rule of lenity. Plaintiffs seek monetary relief under criminal statutes, so "the rule of lenity applies here." *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1182 n.5 (N.D. Cal. 2013); *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). The rule of lenity requires statutory language to be "clear and definite" to "give fair notice" of prohibited conduct, and when in "doubt," courts "must choose the interpretation least likely to impose [unintended] penalties." *See United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012); *see also Bittner v. United States*, 598 U.S. 85, 101 (2023) (resolving case under the rule of lenity, "a venerable principle" providing that "statutes imposing penalties are to be 'construed strictly'"

in favor of defendants). The rationale behind the rule is straightforward: it "not only ensures that citizens will have fair notice of the criminal laws, but also that Congress [and state legislatures] will have fair notice of what conduct its laws criminalize . . . so that [it] will not unintentionally turn ordinary citizens into criminals." *Nosal*, 676 F.3d at 863.

The rule of lenity defeats Plaintiffs' claims. ECPA, CIPA, and CDAFA do not clearly cover the ubiquitous internet tracking technologies challenged in this lawsuit. Neither the text nor the legislative history of those statutes suggests that they were intended to regulate technologies like those at issue here. Had the statutes' drafters intended "to expand the scope of criminal liability to everyone who" uses those ubiquitous technologies, one "would expect it to use language better suited to that purpose." *Id.* at 857. Yet they did not. Multiple courts have recognized as much and have applied the rule of lenity to dismiss claims like the ones Plaintiffs assert here. *See Vita v. New England Baptist Hosp.*, 243 N.E. 3d 1185, 1204–05 (Mass. 2024) (dismissing wiretapping claims because "we are left with serious doubts as to whether browsing and interacting with a public website are a 'wire communication'"); *Gray v. Twitter Inc.*, 2021 WL 11086642, at *8 (W.D. Wash. Mar. 17, 2021) (similar).

Applying the rule of lenity is especially appropriate here, where Plaintiffs' claims are so muddled and confusing. *See, e.g., supra*, Section IV.C; CCAC ¶ 257 (vaguely characterizing the same data as both "content" and "record" information under ECPA and CIPA); *supra*, Section IV.D.2 (discussing Plaintiffs' failure to specify the conduct on which Plaintiffs base their CDAFA claims). And the case for the rule of lenity is even more compelling given the context of TTD's conduct: California has enacted a comprehensive legal regime that legitimatizes and regulates the very activity that Plaintiffs claim exposes TTD to criminal liability, and that conduct is commonplace. *See supra*, Section II.B. Concluding that those technologies violate federal and state criminal statutes would improperly and "unintentionally turn" countless "ordinary citizens into criminals." *Nosal*, 676 F.3d at 863.

F. Plaintiffs have failed to state a claim for unjust enrichment.

Plaintiffs' claim for unjust enrichment fails as a matter of law for at least four reasons. *First*, "in California, there is not a standalone cause of action for 'unjust enrichment.'" *Astiana*,

783 F.3d at 762. *Second*, while unjust enrichment can be construed as a quasi-contract claim, *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016), this requires that the defendant received a benefit at the plaintiff's expense under circumstances, such as "mistake, fraud, coercion, or request," that make it inequitable for the defendant to retain the benefit without paying for its value. *Hammerling*, 615 F. Supp. 3d at 1097. Plaintiffs do not establish a quasi-contractual relationship, mistake, fraud, coercion, or request. CCAC ¶ 157; *see also Griffith v. TikTok, Inc.*, 2023 WL 9019035, at *1, *6 (C.D. Cal. Dec. 13, 2023) (finding "no suggestion" of a "viable quasi-contract theory" where defendant used its software on third-party websites to collect health, financial, religious, and other data about non-users). *Third*, unjust enrichment requires a relationship between the parties. If there is no relationship, or the relationship is too attenuated, there can be no unjust enrichment. *See, e.g.*, *Doe I*, 572 F.3d at 685 ("[T]he lack of any prior relationship between Plaintiffs and [the defendant] precludes the application of an unjust enrichment theory."). Here, Plaintiffs expressly deny any direct relationship with TTD, alleging instead that TTD received data from third parties. CCAC ¶¶ 77, 155, 277. That is insufficient, as courts routinely find. *See, e.g.*, *Katz-Lacabe*, 668 F. Supp. 3d at 946 & n.11 (dismissing claim where plaintiffs "were at no time in direct privity with" the defendant, which received data, if at all, "with permission from the third-party websites"). *Finally*, an unjust enrichment plaintiff must, "at a minimum, *plead* that [it] lack[s] adequate remedies at law." *Guthrie v. Transamerica Life Ins. Co.*, 561 F. Supp. 3d 869, 875 (N.D. Cal. 2021); *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). Plaintiffs have failed to do so and they seek substantial damages.

G. Declaratory judgment is not an independent theory of recovery.

Plaintiffs' independent claim for "appropriate declaratory relief," CCAC ¶ 307, should be dismissed because it is "merely a form of relief" and "does not provide an independent theory for recovery[.]" *Muhammad v. Conner*, 2012 WL 2428937, at *3 (N.D. Cal. June 26, 2012).

V. CONCLUSION

Both the technologies and conduct at issue in this case support the modern internet and enable free content for consumers. Plaintiffs have not plausibly alleged facts showing that these

same technologies and practices are highly offensive, violate Plaintiffs' reasonable expectation of privacy, are prohibited by the multiple criminal statutes Plaintiffs assert claims under, or have unjustly enriched TTD at Plaintiffs' expense.

Plaintiffs' theories of liability would expose countless businesses and ordinary internet users to liability, including criminal exposure, for routine, beneficial activities that occur trillions of times annually across the web. Plaintiffs have failed to state any of their claims. The CCAC should be dismissed.

DATED: September 2, 2025

PERKINS COIE LLP

By: */s/ Susan Fahringer*
Susan Fahringer, Bar No. 162978
Nicola Menaldo (pro hac vice)
PERKINS COIE LLP
1301 Second Avenue, Suite 4200
Seattle, WA 98101
Telephone: 206-359-8687
Fax: 206-359-9000
Email: sfahringer@perkinscoie.com
Email: nmenaldo@perkinscoie.com

Caroline Sundermeyer, Bar No. 353219
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304
Telephone: 650-838-4300
Fax: 650-838-4350
Email: CSundermeyer@perkinscoie.com

Attorneys for Defendant The Trade Desk, Inc.